THE CONTRIBUTION OF E.B. FLEISSNER AND A. FIGL FOR TODAY'S CRYPTOGRAPHY

Otto J. Horak
Armed Forces ADP Agency (HDVA)
A-1070 Vienna, Austria

About two and a half thousands of years ago the antique philosopher HERACLIT has stated that "The war is the father of all things". He was right also for cryptography till to the recent past. Now since some decades business and computer application are perhaps a stronger propulsion for cryptography than military and diplomatic requirements. Therefore on should not wonder that the central figures mentioned here living near the turn of this century were both officers.
Eduard B. FLEISSNER with the full name Eduard Freiherr(baron) von FLEISSNER von WOSTROWITZ, son of an Austrian cavalry captain was born on January 25, 1825 in Lemberg, today capital of Ukrainian Soviet Socialist Republic, at his time part of the Austrian Monarchy. After his education as officer in the famous Theresian Military Academy in Wiener Neustadt (50 km south of Vienna), founded 1752 by the empress Maria Theresia and still even now the academy for Austria officers, he became second lieutenant of the Imperial-Royal Austrian Army in 1843. He advanced continuously, was finally appointed commander of a school for brigade commanders in 1870 and additionally division commander in 1872. In 1874 he retired and moved in 1880 to Vienna where he died on April 29, 1888.

During his work as commander of different military units and especially as teacher on the school for brigade commanders he came in contact with cryptographic means and measures. After his retirement

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 3-17, 1986.

he finished his book on cryptography described later for which he has felt an urgent requirement and which has been published 1881 in Vienna entitled "Handbuch der Kryptographie" (Manual of Cryptography) /1/ (Figure 1). Figure 2 shows the first page of FLEISSNER's personnel file kept in the Austrian Public Record Office/War Record Office (Staatsarchiv/Kriegsarchiv) /2/.

Andreas FIGL was born in Vienna on June 22, 1873 fifteen years before FLEISSNER died. He got his officers education in the cadet school in Trieste, also in the Austrian Monarchy at his time and became lieutenant in 1893. On January 1, 1910 he retired as captain because of defective vision on one eye. Figure 3 shows the first page of his personnel file from this time /2/. One and a half years later he became recommissioned for special services in 1911 and started his career as deciphering officer and cipher specialist. At this time the General Staff of the Austro-Hungarian Army was just establishing a Cryptoanalytic Bureau in the so called Evidenzbüro, an intelligence office, where FIGL was appointed head of this Cryptoanalytic Bureau. After some years at the front during World War I where he was again working in cipher services he became head of the Supreme Army Command Cipher Group from January 1917 till to the end of World War I with an continuous advancement to lieutenant colonel of the Imperial-Royal Austrian Army. After the end of World War I he worked in the new built Staatsamt für Heerwesen (State Agency for Armed Forces Affairs) and advanced 1920 to a colonel. Some time later he changed to civil service in the Federal Police Direction and finally in the Bundeskanzleramt (Federal Chancellor Agency) also responsible for Foreign Affairs where he was working in the cipher group till up to his retirement in July 1937. Nearly ninety-five years old he died on November 11, 1967 in Salzburg, Austria, where he spent the years after his retirement. Soon after World War I new needs for basic cryptographic literature arose. Because FLEISSNER's Book, which fulfilled this task in the past, was sold out FIGL decided to write also a book on cryptography. Entitled "Systeme des Chiffrierens" (Systems of Ciphering) this book was published 1926 in Graz, Austria /3/ (Figure 4).

What are now the contributions of FLEISSNER and FIGL for today's cryptography? The main contributions were their work itself which finds visible expression in the books containing all experience they have collected during their services. Having a look to bibliographies of cryptography like Galland /4/ or Shulman /5/ for the last decades

of the 19th and the first of 20th century there are not to find so much comprehensive manuals like these from FLEISSNER and FIGL. Both books have some in common especially their most impressive quality namely the clear and systematic way in which the authors have mentioned all matter and particular systems as well as they have worked out the difference between ciphering, deciphering and decrypting (unauthorized deciphering) today known as cryptography and cryptoanalysis respectively. Furthermore both authors have announced a second volume of their books but non was ever published. This second volume should mention the area of cryptoanalysis and there FLEISSNER and FIGL found their boundaries, boundaries not in knowledge but in political and military environment. Their time was not yet ready for public scientific cryptoanalysis.

Looking to FLEISSNER's book, about one hundred years old, it is very surprising that his preface translated in today's colloquial language is still true (Figure 5). For example in the first break

> "By the introduction of Post-Correspondence-Cards and the circumstance that encrypted telegrams are allowed in private traffic cryptography or the art of ciphering and deciphering, till now science for few classes, has won significance and interest also for a broader public"

it needs only to exchange the expressions "Post-Correspondence-Cards" and "encrypted telegrams" perhaps by "Credit Cards" and "data communications" respectively and this paragraph will fit for a book on cryptography of the 80s in this century.

Similar is true for the third break where FLEISSNER says that knowledge on cryptography generally is insufficient despite frequent application also in public authorities and professions which should be familiar with cryptography. Therefore they often use cipher methods useless for protecting the secret.

FLEISSNER divided his book in three parts:

I. General on cryptography and preferenced methods,
II. A new grille/transposition cipher (Patronen-Geheimschrift),
III. The art of unauthorized deciphering (cryptanalysis).

The first and third part give a detailed overview on means and methods in these areas based on the knowledge of that time. From the viewpoint of today the second part with the proposed new transposition cipher called "Patronen- Geheimschrift" (Stencil Cipher) is of interest. As "Patrone" (stencil) is to understand a square of cardboard with holes in such an arrangement that by turning 90 degrees around the center to the four possible positions the holes are never on the same place (figure 6). The four sides - proposed with a length of fifteen fields - are designated with 1 to 4 or A to D and on the reverse surface with 5 to 8 or E to H respectively. The character of the cryptogramm in the center hole shows surface and side for starting the encipherment and decipherment. Some complications for security reasons are also described. In the introduction of part II FLEISSNER schedules nine advantages of his new cipher and in number five especially, that this cipher

> "is of extreme security like best other cipher methods only. Science and art are not able to find the key except by a favourable accident what is possible for any cipher".

Furthermore he emphasized the huge variety of possible keys: As known today FLEISSNER is wrong with his new cipher twofold. First the variety depends very on the length of square sides and is additionally limited by the strong regularity necessary to allow turning the square around the center. A further limitation is given with respect to equivalent and weak keys. Second key and cipher device is nearly the same and therefore this "Patrone" has to be kept secret, a condition which hurts very hard the cryptologic axiom that a cipher device must not be secret.

In modesty FLEISSNER stated in his preface that he has written the book as layman for laymen and users and not for specialists. Not so speaks FIGL. Self-confident he believed that a new comprehensive book on cryptography is necessary because all available literature was some decades old, incomplete and unsystematic. Therefore his intention was to collect all his knowledge and practical experience gained in the years of his cryptographic occupation and form it with a strong systematic and scientific structure to a book.

The structure of his book looks like follows:

- Introduction
  - Visible and invisible secret writings,
  - Boundaries and structure of the matter,
  - Special terms,
  - Literature,
- Part I: Letter-Methods
  - Transpositions,
  - Substitutions,
  - Mechanical Methods,
  - Screening,
  - Hiding of writings,
- Part II: Syllable- and Word-Methods
  - Special methods,
  - Key tables (command tables),
  - Book methods.

It is to say that FIGL has not only structured the content very strong he has also worked out all details extremely deep and systematic. Many ancient and at his time more or less well-known methods are described with scientific precision together with their advantages, disadvantages and week points. FIGL described for example already the Enigma cipher machine and in this connection he stated that not the cipher device but only the cipher key is the real cryptographic secret, an axiom hurted by FLEISSNER's "Patronen-Geheimschrift".

Despite the fact that FIGL's book is no longer up-to-date it is cited often also in recent literature because of its fundamental character. Therefore it is not astonishing that the question for his second volume is asked. As already mentioned earlier neither FIGL's nor FLEISSNER's announced second volume were published. Maybe for FLEISSNER the time was to short because he died seven years after publishing the first volume or there was no interest for a second volume on "The Patronen-Geheimschrift (grille/transposition cipher) as word cipher and cryptoanalysis in foreign languages". In case of FIGL the reason is obvious and well documented: The edition of the second volume has been interdicted officially by the same agency where FIGL was working as government official. In 1926 as his book has been published he was with the cipher group in the department for foreign affairs of the Federal Chancellor Agency and he dedicated one copy of his book to the head of this cipher group with a personal inscription. The reaction was horror. The reason is to find in the

way of thinking on secrecy at this time. Some of the methods described by FIGL with its advantages and weaknesses were obviously still in governmental use. Now they are reacting like an oistrich: they rather wanted to keep a week method secret hoping that nobody will detect the weakness than to look for a secure new method. So they were shocked that now the weakness was public. But it was impossible to bring the started arrow back, i.e. to eliminate the already published first volume. Therefore after a contact with the Federal Ministry for Armed Forces Affairs (Bundesministerium für Heerwesen) it was decided to interdict at least the publication of the announced second volume entitled "Systeme des Dechiffrierens" (Cryptoanalysis of Systems). It is known that the second volume was already prepared for printing and that the publisher has been indemnified for the lost copyright. Figure 7 shows the first page of this official document /6/. Furthermore it is said that a typed manuscript should exist based on FIGL's manuscript, written, rearranged and supplemented in some points by a pupil of FIGL.

Concluding the matter mentioned previously it is to ask what can be learned from the work of FLEISSNER and FIGL and the outcome they have initiated with their books. There are three main points worthy to note here:

1. DON'T THINK CRYPTOGRAPHIC NEEDS AND REQUIREMENT ARE KNOWN, UNDERSTOOD AND ACCEPTED EVERYWHERE.

   The remarks in FLEISSNER's preface and the interdiction of FIGL's second volume should illustrate this clear enough.

2. DON'T OVERESTIMATE THE SECURITY OF YOUR OWN SYSTEM.

   FLEISSNER's "Patronen-Geheimschrift" is a splendid negative example. Studying FIGL's book one can find a lot of similar grille ciphers and can be sure that his second volume would have shown a solution.

3. LOOK CAREFULLY WHAT IS TO KEEP SECRET FOR SECURITY REASONS AND WHAT NOT.

   Here again two examples are to count. First FLEISSNER's "Patrone" (stencil): it must not be secret because it is not only a key it

is also a cipher device, second the already mentioned interdiction of FIGL's second volume. Week cipher methods will not become more secure if they will kept secret.

Remembering this points in all situations the work of FLEISSNER and FIGL is not wasted and their contribution for today's cryptography will bear fruits.

References

/1/ FLEISSNER v. WOSTROWITZ Eduard B.
Handbuch der Kryptographie
Seidel & Sohn, Vienna, 1881

/2/ Record files kept in Österreichisches Staatsarchiv/Kriegsarchiv (Austrian Public Record Office/War Record Office), Vienna

/3/ FIGL A.
Systeme des Chiffrierens
Mosers Buchhandlung (J. Meyerhoff), Graz, 1926

/4/ GALLAND Joseph S.
An Historical and Analytical Bibliography of the Literature of Cryptology
Northwestern University, Evanston, 1945

/5/ SHULMAN David
An Annoted Bibliography of Cryptography
Garland Publishing, Inc., New York & London, 1976

/6/ Österreichisches Staatsarchiv/Kriegsarchiv
Number A 49635-1/26

HANDBUCH

der

KRYPTOGRAPHIE.

Anleitung zum Chiffriren

und

Dechiffriren von Geheimschriften.

Von

EDUARD B. FLEISSNER v. WOSTROWITZ
k. k. Oberst.

Mit XIX Tafeln und einer Patrone.

WIEN.
In Selbstverlage des Verfassers. — In Commission bei L. W. Seidel & Sohn.
1881.

FIGURE 1

Qual. Fasc. 725

Truppenkörper: K.k. Graf Grünne Uhlanen Regiment No 1
8.

Name: Eduard Freiherr von Fleißner von Wostrowitz

Charge—Rang: ~~Oberlieutenant / 3ten September 1866~~ / Oberst / 23 [illegible] 1870 [illegible] (VB. 33.)

Geboren: 1825 Lemberg am 25ten Jänner

Religion: katholisch

Persönliche Verhältnisse, Erziehung und Studien vor dem Eintritte in das k. k. Heer:
Sohn eines k.k. Rittmeisters, ohne Vermögen, Zögling der W. Neustädter Militär-Academie

Wann und wie in das k. k. Heer getreten: am 29ten September 1843 als Unterlieutenant aus der W. Neustädter Militär-Academie ausgemustert

Später absolvirte Schulen u. dgl.: /

Privat Verhältnisse:

Jahrgang	
1869	~~verheiratet, Vater von 1 Knaben und 2 Mädchen, ohne Beihilfe, seine Frau besitzt [illegible] und ist [illegible] Leibrente [illegible] – finanziell geordnet –~~
1871	Zu [illegible]
187	

Decorationen:

Inländische:
Militär-Verdienst-Kreuz K. D.
Offiziers-Dienstzeichen 1 Classe
~~[illegible]~~

Fremdländische:

FIGURE 2

4

Truppenkörper: Infanterie Regiment [illegible] Lacy Nr 93

Name: Andreas ~~[illegible]~~ Figl

Charge – Rang: ~~Oberleutnant [illegible] 1896 – Rang Nr 3671~~
~~Hauptmann 2. Kl. [illegible] Mai 1907 – Rang Nr 1171~~

Geboren: in Wien in Niederösterreich am 22 Juni 1873

Heimatszuständig: nach Haslach in Niederösterreich

Religion: römisch katholisch

Persönliche Verhältnisse, Erziehung und Studien vor dem Eintritte in das k. und k. Heer: Sohn eines [illegible], hat durch 3 Jahre das k. u. k. Militär-Knaben-Pensionat in Sarajevo besucht und 1887/88 bis 1888/89 die Infanterie Cadettenschule zu Wien frequentiert und 1889/90 bis 1890/91 die Infanterie Cadettenschule zu Triest mit sehr gutem Erfolge absolviert

Wann und wie in das k. und k. Heer eingetreten: am 18. August 1891 freiwillig auf 3 Linien-, 7 Reserve- und 2 Landwehrjahre zum Infanterie Regimente Graf von Lacy Nr 22 assentiert; hat für die in der Cadettenschule zugebrachte Zeit 4 Jahre über die gesetzliche [illegible] [illegible] nachzudienen. ~~[illegible] bis 22 Juni [illegible]~~

Später absolvierte Schulen u. dgl.: ~~vom 1. Jänner bis 22. Juni 1901 die [illegible] Schule in Agram mit entsprechendem Erfolge absolviert~~

Privat-Verhältnisse:

Jahrgang	
1901	ledig, [illegible] geordnet, ohne Vermögen und ohne Schulden
1	
1	

Decorationen:

Inländische:
Jubiläums-Erinnerungs-Medaille für die bewaffnete Macht.
~~Militärverdienstmedaille am roten Bande~~

Fremdländische:
–

Lag. Nr. 87 a. — Aus der k. k. Hof- und Staatsdruckerei. — IV/1900.

FIGURE 3

4

1003 [illegible]

Wissenschaftliche Veröffentlichungen des Kriminalistischen Laboratoriums der Polizeidirektion Wien
(Wissenschaftl. Vorstand: Dozent Dr. Siegfried Türkel).

SYSTEME DES CHIFFRIERENS

von

A. FIGL
Oberst und Regierungsrat

GRAZ 1926

Verlag von Ulr. Mosers Buchhandlung (J. Meyerhoff)

FIGURE 4

VORWORT.

Durch Einführung der Post-Correspondenz-Karten und durch den Umstand, dass in Geheimschrift abgefasste Telegramme im Privatverkehre gestattet sind, hat die Kryptographie oder die Kunst des Chiffrirens und Dechiffrirens, die bisher die Wissenschaft weniger Stände war, an Bedeutung und Interesse auch für das grössere Publicum gewonnen.

Wenn bisher nur ausschliesslich die Diplomatie und die Generalstäbe der Armeen diese Kunst cultivirten, manchmal auch die grossen Bankhäuser, Kaufherren und Rheder in Verfolgung ihrer Interessen, endlich der Untersuchungsrichter und der Polizeibeamte bei Erfüllung ihres Berufes öfters in die Lage kamen, sich mit der Kryptographie beschäftigen zu müssen, so ist sie jetzt für Jeden, der seine kleinen Geheimnisse nicht einer offenen Post-Correspondenz-Karte anvertrauen will, gewiss von einigem Nutzen.

Da aber die Kenntniss der Kryptographie trotz ihrer vielfältigen Anwendung im Allgemeinen eine sehr ungenügende ist, indem man selbst von staatlichen Behörden und Personen, von denen man schon wegen ihres Berufes eine grössere Vertrautheit mit der Kryptographie voraussetzen sollte, Chiffre-Methoden in Anwendung bringen sieht, die das Geheimniss, also die Hauptsache, nicht sicher zu wahren vermögen, so dürfte ein Werkchen über Kryptographie vielleicht willkommen sein.

Die günstige Beurtheilung, welche das Manuscript zu diesem Buche von Autoritäten erfuhr, bestimmt mich, dasselbe der Oeffentlichkeit zu übergeben.

Von einem Nichtfachmanne geschrieben, ist es nicht für Fachmänner bestimmt, wenn ich auch hoffe, dass selbst diese in meinem Buche manches Neue finden werden. Die Bestimmung desselben ist vielmehr die, dem Laien als treuer Rathgeber bei der Wahl eines verlässlichen Chiffre-Schlüssels zu dienen und dem angehenden Diplomaten, Officier, insbesondere Generalstabs-Officier und überhaupt Allen, deren Beruf sie öfters in die Lage versetzt, von Geheimschriften Gebrauch machen zu müssen, in das weite Gebiet der Kryptographie einzuführen.

Sollte dieses Handbuch den gewünschten Leserkreis finden, so würde ich demselben als zweiten Theil folgen lassen:

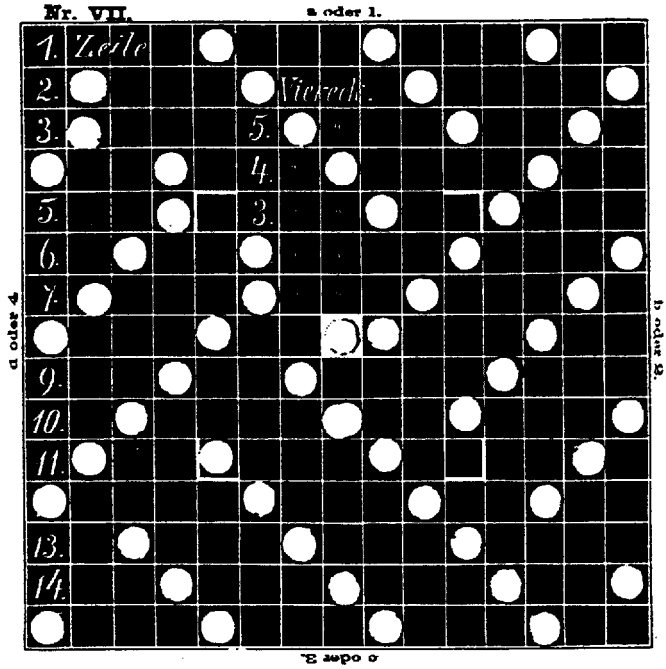
Die Patronen-Geheimschrift als Wort-Chiffre und

Ueber das Dechiffriren in fremden Sprachen, erläutert durch Aufstellung von Regeln, Wörter-Sammlungen und Beispiele für die französische, englische, italienische, russische und ungarische Sprache, damit auch Nichtkenner dieser Sprachen selbe dechiffriren lernen.

Wien, im März 1881.

Der Verfasser.

FIGURE 5



FRONT BACK

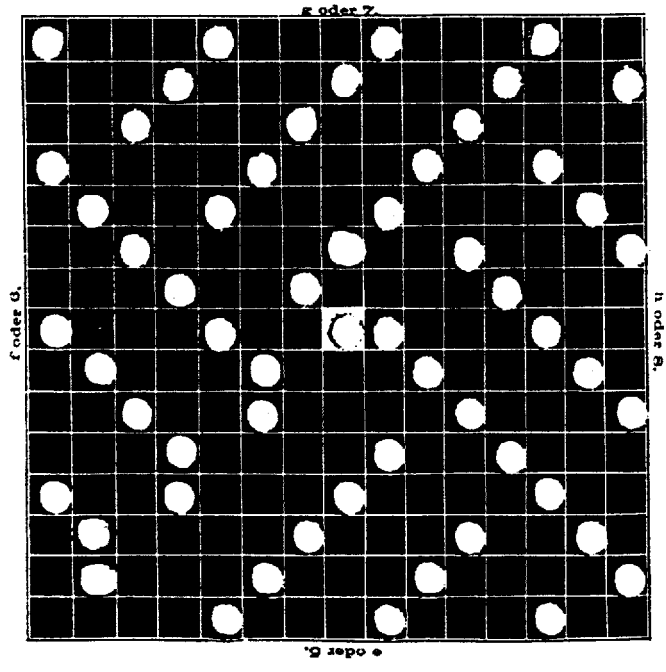


FIGURE 6

Bundesministerium für Heereswesen.

Geschäftszahl 49635 – 1 /1926	Vorzahl	Genehmigungs-, Dringlichkeits- und Verschlußvermerk
Miterledigte Zahlen	Nachzahlen	VERSCHLUSS ! Streng vertraulich. Zur eigenhändigen Eröffnung durch den ~~Präsidialchef.~~ Leiter der Chiffrengruppe (Min Rat. Klob)
	Bezugszahlen	

Gegenstand:	Buchausgabe „ System des Chiffrierens " v. Obst. a.D. FIGL = Antrag auf Verhinderung des Erscheinens weiterer Veröffentlichungen im Gegenstande. *)	Frist / zu betreiben am / neue Frist

Zur Einsicht vor Genehmigung, ~~Abfertigung, Hinterlegung~~

Rechts Büro:

5/XI.

Besonders vertraulich, unter Abteilungsverschluss!

*) TRANSLATION:

Book edition "Systems of Ciphering" by Col.ret. FIGL = Request for Interdiction of edition of further publications in this matter.

KRIEGSARCHIV WIEN

2

Geschäftszeichen	Reing. / Vergl.	9.11.
Grundzahl – /	Begl. / Best.	9.11.

Mil. Lager-Nr. 201. Vortragsbogen. — Druck und Verlag der Österreichischen Staatsdruckerei, D. V., in Wien. (St.) 1552 25

FIGURE 7